

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 2 月 6 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 0 2 8 9 9 8
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 0 2 8 9 9 8]

出 願 人 株式会社ルネサステクノロジ
Applicant(s):

CERTIFIED COPY OF
PRIORITY DOCUMENT

BEST AVAILABLE COPY

2 0 0 4 年 2 月 1 7 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 K03000561A

【あて先】 特許庁長官殿

【国際特許分類】 G06F 12/00

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所システム開発研究所内

 【氏名】 水島 永雅

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所システム開発研究所内

 【氏名】 角田 元泰

【発明者】

 【住所又は居所】 東京都小平市上水本町五丁目 2 0 番 1 号 株式会社日立製作所半導体グループ内

 【氏名】 片山 国弘

【特許出願人】

 【識別番号】 000005108

 【氏名又は名称】 株式会社 日立製作所

【代理人】

 【識別番号】 100075096

 【弁理士】

 【氏名又は名称】 作田 康夫

【手数料の表示】

 【予納台帳番号】 013088

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

【物件名】 要約書 1
【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 メモリカード

【特許請求の範囲】

【請求項 1】

複数のブロックに分割されたメモリと、前記メモリへのアクセスを制御するコントローラと、ＩＣカードチップを備えたメモリカードにおいて、

前記コントローラは、外部のホスト機器からの第１のコマンドに応答して、前記メモリのブロックの利用権を、前記ＩＣカードチップによって実行されるべきアプレットののために前記アプレットごとに割り当て、

前記コントローラは、前記ホスト機器からの第２のコマンドに応答して、前記第１のコマンドに応答した処理を実行可能なアンロック状態から前記第１のコマンドに応答した処理を拒否するロック状態へ遷移するメモリカード。

【請求項 2】

請求項 1 に記載のメモリカードにおいて、

前記メモリは、前記ブロックの識別子と前記ブロックの利用権が割り当てられたアプレットの識別子との対応を管理するための管理情報を記憶可能で、

前記コントローラは、前記アンロック状態である場合に、前記管理情報の内容の変更を許可し、

前記コントローラは、前記ロック状態である場合に、前記管理情報の内容の変更を禁止するメモリカード。

【請求項 3】

請求項 1 に記載のメモリカードにおいて、

前記メモリは、前記ブロックの識別子と前記ブロックの利用権が割り当てられたアプレットの識別子との対応を管理するための管理情報を記憶可能で、

前記コントローラは、前記ブロックの利用権を前記アプレットののために割り当てる場合に、前記ブロックの識別子に対応する前記アプレットの識別子を前記管理情報に追加するメモリカード。

【請求項 4】

請求項 1 に記載のメモリカードにおいて、

前記メモリは、前記第1のコマンドに応答した処理を実行可能か否かを識別するためのフラグを記憶可能で、

前記コントローラは、前記アンロック状態から前記ロック状態へ遷移する場合に、前記フラグの値を変更するメモリカード。

【請求項5】

請求項1に記載のメモリカードにおいて、

前記コントローラは、前記ホスト機器からの第3のコマンドに応答して、前記ロック状態から前記アンロック状態へ遷移するメモリカード。

【請求項6】

請求項5に記載のメモリカードにおいて、

前記メモリは、前記第3のコマンドに応答した処理を許可するための参照パスワードを記憶可能で、

前記コントローラは、前記ホスト機器から受け取ったパスワードと前記メモリ内の前記参照パスワードとが一致した場合に、前記第3のコマンドに応答して、前記ロック状態から前記アンロック状態へ遷移するメモリカード。

【請求項7】

請求項1に記載のメモリカードにおいて、

前記コントローラは、前記ホスト機器からの第4のコマンドに応答して、前記アプレットのために割り当てられた前記ブロックの利用権を解除するメモリカード。

【請求項8】

請求項7に記載のメモリカードにおいて、

前記メモリは、前記ブロックの識別子と前記ブロックの利用権が割り当てられたアプレットの識別子との対応を管理するための管理情報を記憶可能で、

前記コントローラは、前記アプレットのために割り当てられた前記ブロックの利用権を解除する場合に、前記ブロックの識別子に対応する前記アプレットの識別子を前記管理情報から削除するメモリカード。

【請求項9】

請求項1に記載のメモリカードにおいて、

前記メモリは、前記ホスト機器から受け取ったデータを記憶するための第1のエリアと、前記アプレットのために前記ブロックの利用権が割り当てられた第2のエリアとを有するメモリカード。

【請求項10】

請求項9に記載のメモリカードにおいて、

前記コントローラは、前記メモリの前記第2のエリアへ書き込むべきデータを前記ICカードチップから受信し又は前記第2のエリアから読み出されたデータを前記ICカードチップへ送信するための転送コマンドを前記アプレットごとに生成するメモリカード。

【請求項11】

複数のブロックに分割されたメモリと、前記メモリへのアクセスを制御するコントローラと、ICカードチップを備えたメモリカードにおいて、

前記メモリのブロックは、前記ICカードチップによって実行されるアプレットのために前記アプレットごとに割り当てられ、

前記メモリは、前記ICカードチップが前記コントローラへ依頼する外部処理の内容を前記コントローラが前記ICカードチップへ問い合わせるために前記アプレットごとに定められたコマンドを記憶可能で、

前記ICカードチップは、当該ICカードチップが実行すべきアプレットの識別子を前記コントローラへ送出し、

前記コントローラは、前記ICカードチップからの前記アプレットの識別子をキーとして、前記メモリから前記コマンドを読み出し、読み出された前記コマンドを前記ICカードチップへ送出し、

前記ICカードチップは、前記コントローラからの前記コマンドに応答して、前記外部処理の内容を前記コントローラへ通知し、

前記コントローラは、前記ICカードチップからの通知に応答して、前記外部処理を実行するメモリカード。

【請求項12】

請求項11に記載のメモリカードにおいて、

前記コマンドは、前記メモリのブロックへ書き込むべきデータを前記ICカー

ドチップから前記コントローラへ転送するための第1の転送コマンドと、前記メモリのブロックから読み出されたデータを前記コントローラから前記ICカードチップへ転送するための第2の転送コマンドとを含むメモリカード。

【請求項13】

請求項11に記載のメモリカードにおいて、

前記コマンドは、前記アプレットごとに異なり、さらに、外部のホスト機器からのコマンドと異なるメモリカード。

【請求項14】

ICカードチップと、メモリと、前記メモリへのアクセスを制御するコントローラとを備えたメモリカードにおいて、

前記メモリは、外部のホスト機器からのデータを記憶するための第1の記憶エリアと前記ICカードチップからのデータを記憶するための第2の記憶エリアを有し、

前記第2の記憶エリアは、複数のブロックに分割され、

前記各ブロックは、前記ICカードチップによって実行されるべきアプレットのために前記アプレットごとに割り当てられ、

前記コントローラは、前記ホスト機器からのコマンドに応答して前記第1の記憶エリアをアクセスし、

前記コントローラは、前記ICカードチップからのコマンドに応答して前記第2の記憶エリアをアクセスするメモリカード。

【請求項15】

請求項14に記載のメモリカードにおいて、

前記メモリは、前記ブロックの識別子と前記ブロックの利用権が割り当てられたアプレットの識別子との対応を管理するための管理情報を記憶可能であり、

前記コントローラは、前記アプレットの識別子を前記ICカードチップから受信し、受信された前記アプレットの識別子をキーとして前記ブロックの識別子を前記管理情報から決定し、決定された前記ブロックの識別子によって特定されたブロックをアクセスするメモリカード。

【発明の詳細な説明】

【 0 0 0 1 】**【発明の属する技術分野】**

本発明は、セキュリティ機能を搭載した記憶装置及びその記憶装置が挿入可能なホスト機器及びその記憶装置を備えたホスト機器に係り、フラッシュメモリチップとコントローラチップと I C カードチップを有するメモリカード等に関する。

【 0 0 0 2 】**【従来の技術】**

特許文献 1 には、 I C モジュールと大容量のフラッシュメモリを搭載するメモリカードが記載されている。

【 0 0 0 3 】

特許文献 2 には、アプリケーションプログラムごとの実行必須条件を I C カードに記憶させておき、処理要求があった時に実行必須条件を充足していれば実行可能とし、充足していなければ実効不能とすることが記載されている。

【 0 0 0 4 】

特許文献 3 には、 I C カード内のメモリ領域のうち、銀行のために領域 A が、病院のために領域 B が、それぞれ割り付けられていることが記載されている。

【 0 0 0 5 】

【特許文献 1】 特開平 10-198776 号公報

【特許文献 2】 特開 2000-66882 号公報

【特許文献 3】 特開平 6-222980 号公報

【 0 0 0 6 】**【発明が解決しようとする課題】**

しかし、何れの従来技術も、 I C カードのアプリケーションプログラム（アプレット）ごとに、分割された記憶エリアを割り当てることまでは記載されていない。よって、従来技術では、各アプリケーションプログラムが互いのメモリ内のデータを不正に侵害することが懸念される。

【 0 0 0 7 】

本発明の目的は、 I C カードチップのアプレット間のデータ干渉、即ち、一の

アプレットに割り当てられたメモリが他のアプレットにもアクセスされてデータが侵害されることを抑制できる記憶装置を提供することである。

【0008】

【課題を解決するための手段】

本発明は、メモリを複数のブロックに分割し、ブロックの使用権を I C カードチップのアプレットごとに割り当てた。つまり、メモリが、ホスト機器からのデータを記憶するための第 1 の記憶エリア（例えば、ノーマルデータエリア）と I C カードチップからのデータを記憶するための第 2 の記憶エリア（例えば、セキュアデータエリア）を有し、さらに、第 2 の記憶エリアが複数のブロックに分割され、さらに各ブロックがアプレットごとに割り当てられる。

【0009】

また、本発明は、ホスト機器からコマンドによって、ブロックの使用権の割り当て、割り当て解除、割り当て及び解除の禁止、割り当て及び解除の禁止の解除を行うようにした。つまり、本発明は、ホスト機器からの第 1 のコマンド（例えば、アプレット登録コマンド）に応答してメモリのブロックの利用権をアプレットごとに割り当て、ホスト機器からの第 2 のコマンド（例えば、管理テーブルロックコマンド）に応答してアンロック状態からロック状態へ遷移する。さらに、ホスト機器からの第 3 のコマンド（例えば、管理テーブルアンロックコマンド）に応答してロック状態からアンロック状態へ遷移し、ホスト機器からの第 4 のコマンド（例えば、アプレット登録解除コマンド）に応答してアプレットのために割り当てられたブロックの利用権を解除する。

【0010】

また、本発明は、I C カードチップがコントローラへ依頼する外部処理の内容をコントローラが I C カードチップへ問い合わせるためのコマンドを、アプレットごとに規定した。

【0011】

【発明の実施の形態】

以下、本発明の一実施形態について説明する。

【0012】

図1は、本発明を適用したMultiMediaCard (MultiMediaCardはInfineon Technologies AGの登録商標である。以下、「MMC」と略記する。)の内部構成図を簡単に表したものである。MMC110は、MultiMediaCard仕様に準拠するのが好ましい。MMC110は、外部に接続したホスト機器160がMultiMediaCardのプロトコル仕様に準拠したメモリカードコマンドを発行することによって、ファイルデータを読み書きすることができるストレージ機能や、機密データ保護や個人認証などに必要な暗号演算をおこなうことができるセキュリティ処理機能を有する。ホスト機器160は、例えば、携帯電話、携帯情報端末(PDA)、パーソナルコンピュータ、音楽再生(及び録音)装置、カメラ、ビデオカメラ、自動預金預払器、街角端末、決済端末等が該当する。MMC110は、MMC外部端子140、コントローラチップ120、フラッシュメモリチップ130、ICカードチップ150を持つ。フラッシュメモリチップ130は、不揮発性の半導体メモリを記憶媒体とする大容量(例えば、64メガバイト)のメモリチップであり、フラッシュメモリコマンドによりデータの読み書きができる。MMC外部端子140は7つの端子から構成され、外部のホスト機器160と情報交換するために、電源供給端子、クロック入力端子、コマンド入出力端子、データ入出力端子、グランド端子を含む。コントローラチップ120は、MMC110内部の他の構成要素(MMC外部端子140、フラッシュメモリチップ130、ICカードチップ150)と接続されており、これらを制御するマイコンチップである。ICカードチップ150は、ICカードのプラスチック基板中に埋め込むためのマイコンチップであり、その外部端子、電気信号プロトコル、コマンドはISO/IEC 7816規格に準拠している。ICカードチップ150の外部端子には、電源供給端子、クロック入力端子、リセット入力端子、I/O入出力端子、グランド端子がある。ICカードチップ150の外部端子は、グランド端子を除いて、電源供給端子、クロック入力端子、リセット入力端子、I/O入出力端子がコントローラチップ120に接続されている。コントローラチップ120は、ICカードチップ150の外部端子からICカードチップ150にICカードコマンドを発行することによって、外部のホスト機器160から要求されたセ

セキュリティ処理に必要な演算をおこなう。ICカードチップ150は、演算処理を行うためのCPU151と、EEPROM (Electrically Erasable Programmable Read Only Memory) 152とを備える。一方、フラッシュメモリチップ130には、記憶素子を備えるが、マイコンは存在しない。

【0013】

セキュリティ処理は、例えば、ICカードチップ150内のEEPROM152にデータが書き込まれるとき、又は、EEPROM152からデータが読み出されるときにCPU151により実行される。セキュリティ処理の詳細な内容は、EEPROM152内に格納されたプログラムコードによって記述されている。多種多様なセキュリティ処理に適用できるように、そのプログラムコードは機能的に異なる複数のモジュールとして構成されている。CPU151は必要に応じてセキュリティ処理に使用するモジュールを切り替えることができる。以下、このモジュール単位をアプレットと呼ぶ。例えば、EEPROM152は、アプレットA153とアプレットB154とを格納する。EEPROM152の記憶容量は例えば64キロバイトであり、フラッシュメモリチップ130の記憶容量より小さい。但し、本発明を実施する上で、EEPROM152の記憶容量は、フラッシュメモリチップ130の記憶容量と同じでもよいし、大きくてもよい。

【0014】

ICカードチップ150には、セキュリティ評価基準の国際標準であるISO/IEC15408の評価・認証機関によって認証済みである製品を利用する。一般に、セキュリティ処理をおこなう機能を持つICカードを実際の電子決済サービスなどで利用する場合、そのICカードはISO/IEC15408の評価・認証機関による評価と認定を受ける必要がある。MMCにセキュリティ処理をおこなう機能を追加することによってMMC110を実現し、それを実際の電子決済サービスなどで利用する場合、MMC110も同様にISO/IEC15408の評価・認証機関による評価と認定を受ける必要がある。MMC110は、評価・認証機関によって認証済みのICカードチップ150を内蔵し、そのICカードチップ150を利用してセキュリティ処理をおこなう構造を持つことによ

り、セキュリティ処理機能を得る。したがって、MMC 110はISO/IEC 15408に基づくセキュリティ評価基準を容易に満足することができ、MMCにセキュリティ処理機能を追加するための開発期間を短縮することができる。

【0015】

MMC 110は、MultiMediaCard仕様に準拠した外部インタフェースを持つのが好ましい。MMC 110は、一種類の外部インタフェースを通じて、MultiMediaCard仕様に準拠した標準メモリカードコマンドに加えて、セキュリティ処理を実行するコマンド（以下、セキュアライトコマンドと呼ぶ。）を受け付ける。セキュアライトコマンドは入力データを伴う。コントローラチップ120は、MMC 110が受信したコマンドが標準メモリカードコマンドであるか、セキュアライトコマンドであるかによって、アクセスすべきチップを選択し、コマンド処理を分配する機能を持つ。標準メモリカードコマンドを受信したならば、フラッシュメモリチップ130を選択し、これにフラッシュメモリコマンドを発行してホストデータを読み書きできる。また、セキュアライトコマンドを受信したならば、ICカードチップ150を選択し、これにICカードコマンドを発行してセキュリティ処理を実行することができる。ここで発行されるICカードコマンドは、セキュアライトコマンドによって入力されるデータ（以下、セキュアライトデータと呼ぶ。）の中に埋め込まれている。ICカードチップ150はこのコマンドに応じてICカードレスポンスを返すが、コントローラチップ120はそれをキャッシュする。さらに、MMC 110は、一種類の外部インタフェースを通じて、セキュリティ処理の結果を読み出すコマンド（以下、セキュアリードコマンドと呼ぶ。）も受け付ける。セキュアリードコマンドは出力データを伴う。セキュアリードコマンドを受信したならば、キャッシュしておいたICカードレスポンスを含むデータ（以下、セキュアリードデータと呼ぶ。）を出力する。

【0016】

図5は、セキュアライトデータおよびセキュアリードデータのフォーマットの一例を示したものである。このフォーマットは、実行するセキュリティ処理の内容が1つのICカードコマンドで表現でき、セキュリティ処理の結果が1つのI

Cカードレスポンスで表現できる場合に適用することが好ましい。上述の通り、ICカードチップ150に送信するICカードコマンド、ICカードチップ150から受信するICカードレスポンスはともにISO/IEC 7816-4規格に従う。本規格によれば、ICカードコマンドの構成は、4バイトのヘッダ（クラスバイトCLA、命令バイトINS、パラメータバイトP1とP2）が必須であり、必要に応じて、入力データ長指示バイトLc、入力データフィールドDataIn、出力データ長指示バイトLeが後に続く。また、ICカードレスポンスの構成は、2バイトのステータスSW1とSW2が必須であり、必要に応じて、出力データフィールドDataOutがその前に置かれる。本フォーマットにおけるセキュアライトデータ501は、ICカードコマンド502の前にICカードコマンド長Lc a 504を付け、さらにICカードコマンド502の後にダミーデータ505をパディングしたものである。Lc a 504の値はICカードコマンド502の各構成要素の長さを合計した値である。一方、セキュアリードデータ511は、ICカードレスポンス512の前にICカードレスポンス長Lr a 514を付け、さらにICカードレスポンス512の後にダミーデータ515をパディングしたものである。Lr a 514の値はICカードレスポンス512の各構成要素の長さを合計した値である。なお、この図では、ICカードコマンドにLc、DataIn、Leが含まれ、ICカードレスポンスにDataOutが含まれる場合のフォーマット例を表している。MMC 110に対する標準メモリカードコマンドに含まれるデータリード/ライトコマンドの仕様では、リード/ライトアクセスするデータを固定長のブロック単位で処理することが基本となっている。よって、セキュアライトデータ501やセキュアリードデータ511のサイズも、MMC 110の標準メモリカードコマンドの仕様に準拠したブロックサイズに一致させることが好ましい。ダミーデータ505、515は、セキュアライトデータ501やセキュアリードデータ511のサイズをブロックサイズに一致させるために適用される。ブロックサイズとして採用する値は、一般の小型メモリカードが論理ファイルシステムに採用しているFAT方式におけるセクタサイズ（512バイト）が望ましい。パディングするダミーデータ505、515は全てゼロでもよいし、乱数でもよいし、コントローラチップ120や

ホスト機器 160 がデータエラーを検出したり訂正するためのチェックサムでもよい。L c a 5 0 4 の値はコントローラチップ 120 がセキュアライトデータ 501 からダミーデータ 505 を除去して IC カードコマンド 502 を抽出するために使用し、L r a 5 1 4 の値はホスト機器 160 がセキュアリードデータ 511 からダミーデータ 515 を除去して IC カードレスポンス 512 を抽出するために使用する。

【0017】

コントローラチップ 120 は、電源供給端子、クロック入力端子を通して、IC カードチップ 150 への電源供給、クロック供給を制御する。ホスト機器 160 からセキュリティ処理を要求されないときには、IC カードチップ 150 への電源供給やクロック供給を停止させることができ、MMC 110 の電力消費を削減することができる。

【0018】

電源供給されていない IC カードチップ 150 を、IC カードコマンドを受信できる状態にするには、まず、IC カードチップ 150 に電源供給を開始し、リセット処理を施すことが必要である。コントローラチップ 120 は、MMC 110 がホスト機器 160 からセキュアライトコマンドを受信したのを契機に、電源供給端子を通して IC カードチップ 150 への電源供給を開始する機能を持つ。また、コントローラチップ 120 は、MMC 110 がホスト機器 160 からセキュアライトコマンドを受信したのを契機に、リセット入力端子を通して IC カードチップ 150 のリセット処理をおこなう機能を持つ。コントローラチップ 120 は、セキュアライトコマンドを受信するまで IC カードチップ 150 への電源供給を停止させておくことができる。したがって、MMC 110 の電力消費を削減することができる。

【0019】

コントローラチップ 120 は、IC カードチップ 150 のクロック入力端子を通して IC カードチップ 150 に供給するクロック信号を MMC 110 内部で発生し、その周波数、供給開始タイミング、供給停止タイミングを制御する機能を持つ。MMC 外部端子 140 のクロック入力端子のクロック信号と無関係にする

ことができるため、ホスト機器 160 によるタイミング解析、電力差分析、故障利用解析と呼ばれる攻撃法に対してセキュリティが向上する。

【0020】

フラッシュメモリチップ 130 は、ノーマルデータエリア 131 と管理エリア 132 とセキュアデータエリア 133 とを含む。

【0021】

ノーマルデータエリア 131 は、セクタ単位に論理アドレスがマッピングされている領域であり、ホスト機器 160 が標準メモリカードコマンドを使用することにより指定した論理アドレスにデータを読み書きできる領域である。

【0022】

セキュアデータエリア 133 は、IC カードチップ 150 内の EEPROM 152 に格納されたアプレット（例えば、153 や 154）を CPU 151 が実行する際に（すなわち、セキュリティ処理を実行する際に）、扱うデータを格納することができる領域である。セキュアデータエリア 133 は複数のブロックに分割されている。これをセキュアデータブロックと呼ぶ。例えば、セキュアデータエリア 133 は 4 つのセキュアデータブロック 133 a、133 b、133 c、133 d で構成される。セキュアデータブロックは、コントローラチップ 120 がアプレットごとにその利用権を割り当てることができる単位である。例えば、アプレット A 153 はセキュアデータブロック c 133 c の利用権を持ち、アプレット B 154 はセキュアデータブロック a 133 a の利用権を持つ。また、各セキュアデータブロックは複数の固定長データレコードに分割されている。例えば、1 レコードのサイズは 128 バイトであり、1 つのセキュアデータブロック当たり 8192 個のレコードで構成される。このとき、1 つのセキュアデータブロックのサイズが 1 メガバイトとなり、セキュアデータエリア 133 の容量は 4 メガバイトとなる。したがって、EEPROM 152 に格納されたアプレットは、セキュアデータエリア 133 に格納されたデータにアクセスすることによって、EEPROM 152 の容量以上の不揮発データを利用できる。例えば、IC カードチップ 150 内のアプレット A 153 が電子決済に関するセキュリティ処理のためのプログラムである場合、決済ログ（支払金額や日時など）をセキュアデ

ータエリア 133 に格納することにより、EEPROM 152 のみを利用するよりも多くの決済ログが保存でき、ユーザの利便性が高くなる。IC カードチップ 150 からセキュアデータエリア 133 へのアクセス方法の詳細は後に述べる。

【0023】

一方、管理エリア 132 は、コントローラチップ 120 がセキュアデータエリア 133 を管理するための情報を格納する領域である。コントローラチップ 120 は、MMC 110 がホスト機器 160 からセキュアライトコマンドを受信したことを契機に、この領域に情報を格納したり、削除したりする。そのコマンドについては後述する。管理エリア 132 は、ロックフラグ 134 とパスワードエリア 135 と管理テーブル 136 とを含む。

【0024】

管理テーブル 136 は、セキュアデータエリア 133 を構成している各セキュアデータブロックの利用権を持つアプレットを登録するための領域である。アプレットを識別するために、この領域にアプリケーション識別子（以下、AID (Application Identifier) と呼ぶ。）を格納することによってアプレットを登録することが望ましい。AID は、IC カードのアプリケーションプログラムを識別するために、国際的にユニークに割り振られた値を持つ。国際的に流通する AID の付番方法は、国際規格として ISO/IEC 7816-5 で規定されている。AID を利用することにより、セキュアデータエリア 133 を使用するアプレットを確実に識別することができる。コントローラチップ 120 は、AID 137 に同一の AID を複数格納することを禁止する。管理テーブル 136 のブロックの欄は、セキュアデータブロックを識別するためのブロック識別子としてブロックの先頭アドレス値を登録する。但し、先頭アドレス値の代わりに MMC 内でユニークな番号をブロック識別子として登録してもよい。尚、管理テーブル 136 の代わりに、各セキュアデータブロック内に直接に AID を登録) してもよい。

【0025】

管理テーブル 136 には、AID 137 だけでなく、アプレットごとに転送コマンドコード 138 を格納することができる。この転送コマンドコード 138 は

、コントローラチップ120がセキュアデータブロックの利用権を、アプレットのために割り当てる時に、コントローラチップ120によって生成されるのは好ましい。転送コマンドコードとは、“ライト転送コマンド” および “リード転送コマンド” それぞれのコマンドAPDU (Application Protocol Data Unit) のCLAバイトとINSバイトに設定する2バイト×2個の値である。ここで、“ライト転送コマンド” および “リード転送コマンド” とは、セキュアデータエリア133にレコードデータをライトする前、あるいはそこからレコードデータをリードした後に、コントローラチップ120とICカードチップ150との間でそのレコードデータを転送するために、コントローラチップ120がICカードチップ150に対して発行するICカードコマンド形式のコマンドである。特に、コントローラチップ120へレコードデータを送り出すためのコマンドをライト転送コマンドと呼び、ICカードチップ150へレコードデータを送り込むためのコマンドをリード転送コマンドと呼ぶ。これらのコマンドの詳細な説明は後述する。セキュアデータエリア133の利用権を持つアプレット(153や154)には、ライト／リード転送コマンドを受信した際にレコードデータを扱う処理プログラムが記述されている。転送コマンドコード138はアプレットごとに個別に決められるようになっている。もし、転送コマンドコードが全てのアプレットに共通の固定値であるならば、ホスト機器160からのセキュアライトデータに含まれるアプレット特有のコマンドとライト／リード転送コマンドとの間でコーディングの競合が発生する可能性がある。本発明によれば、このようなコーディング競合を防ぐことができる。なお、転送コマンドコード138のうちINSコードに関しては、伝送プロトコルの都合上ISO/IEC 7816-3に準拠していなければならない。

【0026】

ロックフラグ134は、管理テーブル136に格納された登録情報の変更の可否を示す1バイトのデータを格納する領域である。この領域にFFhを設定することで管理テーブル136の情報の変更が禁止状態(ロック状態)であることを示す。また、00hを設定することで管理テーブル136の情報の変更が許可状態(アンロック状態)であることを示す。

【 0 0 2 7 】

パスワードエリア 1 3 5 は、管理テーブル 1 3 6 の情報をアンロック状態にするための 2 5 5 バイトのパスワードの参照値を格納しておく領域である。管理テーブル 1 3 6 の情報をロックする時には必ず、ホスト機器 1 6 0 からセキュアライトコマンドにより、2 5 5 バイトのパスワード参照をこの領域に設定する。管理テーブル 1 3 6 の情報をアンロック状態にする場合は、ホスト機器 1 6 0 からセキュアライトコマンドにより、ロック時に設定したパスワード参照と同じパスワードを入力する必要がある。入力したパスワードとパスワード参照との一致によって、管理テーブル 1 3 6 の情報の変更をアンロックすることができる。

【 0 0 2 8 】

管理エリア 1 3 2 は、ホスト機器 1 6 0 が不正にアクセスしてセキュリティ処理を解析することができないように、コントローラチップ 1 2 0 により物理的にアクセス制限がかけられている。つまり、管理エリア 1 3 2 はコントローラチップ 1 2 0 による論理アドレスが割り振られていないため、ホスト機器 1 6 0 が直接データを読み書きできない。したがって、MMC 1 1 0 のセキュリティ処理の信頼性や安全性が向上する。

【 0 0 2 9 】

以下、図 2 を参照しながら、セキュアデータエリア 1 3 3 に対するレコードデータのライト／リードアクセスにおいて用いられるライト／リード転送コマンドのコマンド A P D U とレスポンス A P D U について詳細に述べる。

【 0 0 3 0 】

図 2 a は、I C カードチップ 1 5 0 が出力するレスポンス A P D U を示している。このレスポンス A P D U 2 0 0 に含まれる D a t a O u t 2 0 4 の先頭 2 バイト（以下、先頭から順に第 1 制御バイト 2 0 1、第 2 制御バイト 2 0 2 と呼ぶ。）、および S W 1 バイト 2 0 5 と S W 2 バイト 2 0 6 に特別な値を設定することにより、I C カードチップ 1 5 0 はコントローラチップ 1 2 0 にセキュアデータエリア 1 3 3 に対するアクセス要求を通知することができる。なお、後続出力データ 2 0 3 （D a t a O u t 2 0 4 のうち第 1 制御バイト 2 0 1 と第 2 制御バイト 2 0 2 を除いた部分）は、アクセス要求に必要な情報を送信するために使用

される。

【0031】

ICカードチップ150は、コントローラチップ120に対してセキュアデータエリア133へアクセスすることを要求するため、SW1バイト205とSW2バイト206に90FFhという専用のステータス値を設定しなければならない。コントローラチップ120は、ICカードチップ150が出力するレスポンスAPDUを常に監視し、SW1バイト205とSW2バイト206の値が90FFhであることを検出したら、その前方にあるDataOut204の第1制御バイト201、第2制御バイト202第1制御バイト第2制御バイトを調査し、要求されたアクセスの内容などを認知する。一方、90FFhでなかった場合は、このレスポンスAPDUを含むセキュアリードデータをホスト機器160に出力する。ただし、SW1バイト205とSW2バイト206の値が90FFhであっても、条件によって、そのままホスト機器160に出力されることがある。その詳細は後述する。

【0032】

コントローラチップ120は、セキュアデータエリア133へのアクセスを開始するとき、ICカードチップ150上で選択されているアプレットが何であるかによって、133a~133dの中からアクティブにするセキュアデータブロックを選択する。アクセスすべきセキュアデータブロックの選択は、ICカードチップ150からアクセス開始要求が発生した直後におこなう。アクセス開始要求のためにDataOut204に設定するデータの仕様を以下に示す。第1制御バイト201の上位4ビットには、0001を設定する。第1制御バイト201の下位4ビットには、アクセスモードを示すコードを設定する。ここで指定可能なアクセスモードには、レコードデータのライト、レコードデータのリードの2種類がある。0001というコードはレコードデータのライト、0010というコードはレコードデータのリードである。その他のコードは無効である。また、後続出力データ203には、ICカードチップ150上で選択されているアプレットのAIDを設定する。第2制御バイト202には、そのAIDの長さを設定する。

【0033】

コントローラチップ120は、第1制御バイトの上位4ビットが0001ならば、後続出力データ203に含まれるAIDで管理テーブル136内の全てのAID137を検索し、アクティブにすべきセキュアデータブロックを決定する。一致するAIDが見つからなかった場合は、このレスポンスAPDUを含むセキュアリードデータをホスト機器160に出力する。AIDを検出し、それに対応するセキュアデータブロックが判明した後、コントローラチップ120は、第1制御バイトの下位4ビットが0001ならばライト、0010ならばリードのアクセスを開始すると認識する。第1制御バイトの下位4ビットがそれ以外の場合は、このレスポンスAPDUを含むセキュアリードデータをホスト機器160に出力する。

【0034】

コントローラチップ120がアクセスモード（ライトまたはリード）を認知した後、そのモードに応じてライト／リード転送コマンドを発行することによって、アクティブなセキュアデータブロックに対してライトすべきレコードデータ、またはリードしたレコードデータをICカードチップ150とコントローラチップ120との間で転送することができる。図2bと図2cはライト／リード転送コマンドのコマンドAPDUを示したものである。図2bはコントローラチップ120からICカードチップ150への転送データがない場合、図2cは転送データがある場合を示している。前述のように、ライト／リード転送コマンドのコマンドAPDU210（または220）のCLAバイト214（または226）とINSコード215（または227）にはあらかじめアプレットごとに登録されたものを設定する。そのため、管理テーブル136から2バイト×2個の転送コマンドコード138を読み出す。

【0035】

ライト／リード転送コマンドのコマンドAPDU210（または220）では、直前のアクセスの結果をICカードチップ150に通知するため、P1バイト216（または228）とP2バイト217（または229）に特殊な値を設定する。0000hは直前のアクセスにエラーがないことを意味する。80XXh

は直前のアクセスにエラーが発生したことを意味する。なお、XXはエラー内容を示す16進コードである。エラーの場合、アクティブなセキュアデータブロックへのデータアクセスは実行されない。よって、セキュアデータブロックのレコードデータの内容も変化しない。

【0036】

ICカードチップ150は、ライト／リード転送コマンドのレスポンスAPDU 200における後続出力データ203を用いて、ライトしたいレコード番号とレコードデータ、またはリードしたいレコード番号をコントローラチップ120に送信する。ライトモードでは、指定レコード番号（4バイト）とライトデータ（128バイト）の連結データを設定し、リードモードでは、指定レコード番号（4バイト）を設定する。このように、後続出力データ203の長さはアクセスモードによって変わるので、ライト／リード転送コマンドのコマンドAPDUのLeバイト213（または225）には、アクセスモードに応じた値を設定する必要がある。ライトモードでは、後続出力データ203の長さが84hとなるのでDataOut204の長さは86hとなる。よって、Leバイト213（または225）には86hを設定する。リードモードでは、後続出力データ203の長さが04hとなるのでDataOut204の長さは06hとなる。よって、Leバイト213（または225）には06hを設定する。

【0037】

アクセス開始直後の（つまり、最初に発行される）ライト／リード転送コマンドのコマンドAPDUは、図2bの形式となる。そのとき、P1バイト216とP2バイト217には、0000hを設定する。Leバイト213には、ライトモードの場合86hを、リードモードの場合06hを設定する。

【0038】

ライト／リード転送コマンドのレスポンスAPDUは、図2aの形式をとる。ICカードチップ150上で選択されているアプレットは、レスポンスAPDU 200を利用してアクティブなセキュアデータブロックに対するアクセス（ライト／リード）をコントローラチップ120に要求することができる。以下、これをアクセス実行要求と呼ぶ。第1制御バイト201と第2制御バイト202に設

定するデータの仕様を以下に示す。第1制御バイト201の上位4ビットには、0010を設定する。第1制御バイト201の下位4ビットには、要求するアクセスを示すコードを設定する。0001というコードはレコードデータのライト、0010というコードはレコードデータのリードである。その他のコードは無効である。このコードが表すアクセスモードは、コントローラチップ120が認めるアクセスモードに一致していなければならない。また、その第2制御バイト202によって、次のアクセスモード（ライト／リード）の要求をおこなうことができる。コントローラチップ120はこれを参照して、自身が認めるアクセスモードをスイッチする。

【0039】

コントローラチップ120は、第1制御バイト201の上位4ビットが0010ならば、アクティブなセキュアデータブロックに対して、指定されたレコード番号のデータをライト／リードする。ライト／リード処理が正常終了した場合（アクセス結果212（または222）の値が0000h）、第2制御バイト202が01hならば自身が認めるアクセスモードをライトモードにスイッチ、02hならばリードモードにスイッチする。ライト／リード処理に何らかのエラーがあった場合（アクセス結果212（または222）の値が80XXh）、自身が認めるアクセスモードをスイッチせずにエラーが起きた時点のものを維持する。

【0040】

コントローラチップ120が2回目以降に発行するライト／リード転送コマンドのコマンドAPDUは、直前のアクセスの結果やアクセスモードの状態遷移によって、図2bの形式になったり、図2cの形式になったりする。またLe213（または225）の値も変わる。その詳細を以下に示す。

【0041】

直前のライトアクセスが正常で次回もライトモードのとき、図2bの形式であり、アクセス結果212の値が0000hで、Le213の値は86hである。

【0042】

直前のライトアクセスが正常で次回がリードモードのとき、図2bの形式であり、アクセス結果212の値が0000hで、Le213の値は06hである。

【0 0 4 3】

直前のリードアクセスが正常で次回もリードモードのとき、図 2 c の形式であり、アクセス結果 2 2 2 の値が 0 0 0 0 h で、L c 2 2 3 の値は 8 0 h で、D a t a I n 2 2 4 にはリードしたレコードデータが設定され、L e 2 2 5 の値は 0 6 h である。

【0 0 4 4】

直前のリードアクセスが正常で次回がライトモードのとき、図 2 c の形式であり、アクセス結果 2 2 2 の値が 0 0 0 0 h で、L c 2 2 3 の値は 8 0 h で、D a t a I n 2 2 4 にはリードしたレコードデータが設定され、L e 2 2 5 の値は 8 6 h である。

【0 0 4 5】

直前のライトアクセスがエラーのとき、図 2 b の形式であり、アクセス結果 2 1 2 の値が 8 0 X X h で、L e 2 1 3 の値は 8 6 h である。

【0 0 4 6】

直前のリードアクセスがエラーのとき、図 2 b の形式であり、アクセス結果 2 1 2 の値が 8 0 X X h で、L e 2 1 3 の値は 0 6 h である。

【0 0 4 7】

アクセスエラー時にアクセス結果 2 1 2 （または 2 2 2 ）に設定する 8 0 X X h において、エラー内容を示すコード X X の例を以下に示す。

【0 0 4 8】

X X = 0 1 は、指定されたレコード番号がアクセス可能な範囲外であるエラーを意味する。

【0 0 4 9】

X X = 0 2 は、フラッシュメモリチップ 1 3 0 が故障などにより利用できないエラーを意味する。

【0 0 5 0】

X X = 0 3 は、第 1 制御バイト 2 0 1 の下位 4 ビットが現在のアクセスモードに合致しないエラーを意味する。

【0 0 5 1】

XX=04は、第2制御バイト202で要求された次のアクセスモードが不正であるエラーを意味する。

【0052】

図3を参照しながら、ICカードチップ150内のアプレットが、セキュアデータエリア133にアクセスを開始するときの処理の流れ、およびライト／リード転送コマンドによってそこに対するアクセスを実行するときの処理の流れを説明する。

【0053】

ホスト機器160はMMC110にセキュアライトコマンドを発行し(301)、セキュアライトデータ501を入力する(302)。コントローラチップ120は、セキュアライトデータ501からICカードコマンドのコマンドAPDU502を抽出し(303)、それを用いてICカードチップ150にICカードコマンドを発行する(304)。

【0054】

ICカードチップ150は、そのICカードコマンドを受信し(305)、セキュアデータエリア133へのアクセスを要求するICカードレスポンス200を作成し、それを返信する(306)。コントローラチップ120は、このレスポンスを受信し、そのSW1バイト205とSW2バイト206が90FFhであるかを調べる(307)。90FFhでないならばステップ308に移る。90FFhであるならば、第1制御バイト201の上位4ビットが0001(アクセス開始要求)であるかを調べる(312)。0001でないならばステップ320に移る。0001であるならば、管理テーブル136がロックされているか調べる(313)。アンロックされているならばステップ308に移る。ロックされているならば、後続出力データ203に含まれるAIDで管理テーブル136上のAID137を検索する(314)。一致するAIDを検出したならば(315)、コントローラチップ120はアクセス開始要求を承認し、ステップ316に移る。検出しなければアクセス開始要求を却下し、ステップ308に移る。ステップ316では、検出したAID137に対応するセキュアデータブロックを選択し、それをアクティブにする。さらに、対応する転送コマンドコード1

38を取得する(317)。そして、第1制御バイト201の下位4ビットを調べて、開始するアクセスモードを取得し(318)、そのアクセスモードに応じて図2bに示すようなライト／リード転送コマンドを作成する(319)。その後、ステップ304に戻り、ICカードチップ150にライト／リード転送コマンドを発行する。

【0055】

ステップ320では、第1制御バイト201の上位4ビットが0010(アクセス実行要求)であるかを調べる。0010でないならばステップ308に移る。0010であるならば、アクティブなセキュアデータブロックが存在するか、また第1制御バイト201の下位4ビットがコントローラチップ120の認知するアクセスモードに合致するかを調べる(321)。いずれかが偽ならばステップ308に移る。両者とも真ならば、アクセス実行を承認し、後続出力データ203に含まれるレコード番号を取得する(322)。そして、そのレコード番号の指示するデータに対してライト／リードを実行する(323)。このとき、ライトモードの場合は、後続出力データ203に含まれる128バイトのデータをライトする。次に、そのアクセスの結果を示すコードを212または222に設定する(324)。そして、第1制御バイト201の下位4ビットを調べて、次のアクセスモードを取得し(318)、そのアクセスモードに応じて図2bまたは図2cに示すようなライト／リード転送コマンドを作成する(319)。その後、ステップ304に戻り、ICカードチップ150にライト／リード転送コマンドを発行する。

【0056】

ステップ308では、ICカードチップ150が返信したレスポンスAPDU 512からセキュアリードデータ511を作成する。ステップ308に至ることによって、セキュアデータエリア133へのアクセスは終了する。この後、ホスト機器160はセキュアリードコマンドを発行し(309)、コントローラチップ120はセキュアリードデータ511を出力する(310)。そして、ホスト機器160はセキュアリードデータ511を受信する(311)。

【0057】

以上より、ホスト機器 1 6 0 から一組のセキュアライト／セキュアリードコマンドを MMC 1 1 0 に処理させる間に、IC カードチップ 1 5 0 内のアプレットは任意の回数、セキュアデータエリア 1 3 3 へアクセスすることができる。

【0 0 5 8】

以下、管理エリア 1 3 2 に関するアクセスについて説明する。

【0 0 5 9】

ホスト機器 1 6 0 が管理エリア 1 3 2 の情報にアクセスできるように、MMC 1 1 0 は、以下の 4 つの管理コマンドに応じることができる。すなわち、(1) アプレット登録コマンド、(2) アプレット登録解除コマンド、(3) 管理テーブルロックコマンド、(4) 管理テーブルアンロックコマンドの 4 つである。(1) は、管理テーブル 1 3 6 にセキュアデータエリア 1 3 3 を利用するアプレットを登録し、アプレットが利用するセキュアデータブロックを割り当てるコマンド、(2) は、管理テーブル 1 3 6 からアプレットの登録情報を削除し、セキュアデータブロックの割り当てを解除するコマンド、(3) は、管理テーブル 1 3 6 上の登録情報の変更を禁止するコマンド、(4) は、管理テーブル上 1 3 6 の登録情報の変更を許可するコマンドである。これらのコマンドは、一般のセキュリティ処理と同じくセキュアライトコマンドとセキュアリードコマンドのプロトコルによって実施され、コントローラチップ 1 2 0 によって処理される。また、その際に入出力されるセキュアライトデータとセキュアリードデータに含まれる APDU (図 5 における 5 0 2 や 5 1 2) を利用して各処理(登録、登録解除、ロック、アンロック)に必要な情報を交換する。

【0 0 6 0】

アプレット登録コマンドとアプレット登録解除コマンドでは、Data In 5 0 6 に AID を設定する。この AID によって登録したいアプレットを指定する。AID とセキュアデータブロックとをどのように対応付けるかはコントローラチップ 1 2 0 が決定する。ホスト機器 2 2 0 はセキュアデータブロックを直接指定できない。

【0 0 6 1】

管理テーブルロックコマンドでは、Data In 5 0 6 に 2 5 5 バイトのパス

ワードを設定する。そのパスワードはパスワードエリア 1 3 5 に設定され、ロックフラグ 1 3 4 が F F h (ロック状態) になる。これにより、アプレット登録コマンドとアプレット登録解除コマンドが無効になる。すでにロック状態だった場合は、そのパスワードはパスワードエリア 1 3 5 に設定されず、アプレット登録コマンドとアプレット登録解除コマンドは有効のままとなる。

【0 0 6 2】

管理テーブルアンロックコマンドでは、D a t a I n に 2 5 5 バイトのパスワードを設定する。そのパスワードはパスワードエリア 1 3 5 に設定された値と一致比較され、一致したならばロックフラグ 1 3 4 が 0 0 h (アンロック状態) になる。これにより、アプレット登録コマンドとアプレット登録解除コマンドが有効になる。すでにアンロック状態だった場合は、アプレット登録コマンドとアプレット登録解除コマンドは無効のままとなる。

【0 0 6 3】

アプレット登録コマンドとアプレット登録解除コマンドが有効な状態 (アンロック状態) では、パスワードを知らないホスト機器 1 6 0 によって管理テーブル 1 3 6 の情報が不正に変更され、あるアプレットが、それ自身がアクセス可能なセキュアデータブロック以外のセキュアデータブロックをライト／リードするという不正アクセスが発生しうる。そこで、コントローラチップ 1 2 0 は、ロックフラグ 1 3 4 の値が 0 0 h (アンロック状態) では、I C カードチップ 1 5 0 内で選択されているアプレットがセキュアデータエリアへアクセスするのを許可しない。ホスト機器 1 6 0 は、管理テーブル 1 3 6 の登録情報の設定／変更後は、管理テーブルロックコマンドにより必ずロックフラグ 1 3 4 を F F h に設定しなければならない。

【0 0 6 4】

図 4 を参照しながら、上記 4 つの管理コマンドの処理の流れを説明する。

【0 0 6 5】

ホスト機器 1 6 0 は MMC 1 1 0 にセキュアライトコマンドを発行し (4 0 1)、セキュアライトデータ 5 0 1 を入力する (4 0 2)。コントローラチップ 1 2 0 は、セキュアライトデータ 5 0 1 から I C カードコマンドのコマンド A P D

U502を抽出し(403)、それが管理コマンドであるかを調べる(404)。管理コマンドならばステップ407に移る。一方、管理コマンドでないならば、そのコマンドAPDU502を用いてICカードチップ150にICカードコマンドを発行し(405)、ICカードチップ150からそのレスポンスを受信し(406)、ステップ427に移る。

【0066】

ステップ407では、コントローラチップ120は、コマンドAPDU502がアプレット登録コマンドを示すものかを調べる。アプレット登録コマンドならばステップ411に移る。さもなくば、それがアプレット登録解除コマンドを示すものかを調べる(408)。アプレット登録解除コマンドならばステップ412に移る。さもなくば、それが管理テーブルロックコマンドを示すものかを調べる(409)。管理テーブルロックコマンドならばステップ413に移る。さもなくば、それが管理テーブルアンロックコマンドを示すものかを調べる(410)。管理テーブルアンロックコマンドならばステップ414に移る。さもなくば、ステップ425に移る。

【0067】

ステップ411では、ロックフラグ134を見て、管理テーブル136がアンロック状態かを調べる。ロック状態ならばステップ425に移る。アンロック状態ならば、DataIn506内のAIDと同一のものが既に登録されているAID137の中に存在するか調べる(415)。存在していればステップ425に移る。存在しなければ、管理テーブル136上に空きがあるか(つまり、まだ割り当てられていないセキュアデータブロックが存在するか)を調べる(416)。空きがなければステップ425に移る。空きがあれば、そのセキュアデータブロックに対応するAID137と転送コマンドコード138に、DataIn506に含まれるAIDと転送コマンドコードを設定する(417)。これにより、AIDで示されたアプレットがそのセキュアデータブロックの利用権を獲得する。そして、ステップ426に移る。

【0068】

ステップ412では、ロックフラグ134を見て、管理テーブル136がアン

ロック状態かを調べる。ロック状態ならばステップ425に移る。アンロック状態ならば、DataIn506内のAIDで、登録されている全てのAID137の中を検索する(418)。一致するAIDを検出したならば(419)、管理テーブル136上からそのAID137とそれに対応する転送コマンドコード138を削除する(420)。一致するAIDを検出しなければステップ425に移る。これにより、AIDで示されたアプレットがそのセキュアデータブロックの利用権を失う。そして、ステップ426に移る。

ステップ413では、ロックフラグ134を見て、管理テーブル136がアンロック状態かを調べる。ロック状態ならばステップ425に移る。アンロック状態ならば、ロックフラグ134にFFhを設定し(421)、管理テーブル136をロック状態にする。DataIn506内のパスワードをパスワードエリア135に設定する(422)。そして、ステップ426に移る。

【0069】

ステップ414では、ロックフラグ134を見て、管理テーブル136がアンロック状態かを調べる。アンロック状態ならばステップ425に移る。ロック状態ならば、DataIn506内のパスワードがパスワードエリア135に設定したものと一致するかを調べる(423)。一致しないならば、ステップ425に移る。一致するならば、ロックフラグ134に00hを設定し(424)、管理テーブル136をアンロック状態にする。そして、ステップ426に移る。

【0070】

ステップ425では、管理コマンドの処理でエラーが発生したことをホスト機器160に示すため、エラー内容を示すステータスコードを含むレスポンスAPDU512を作り、ステップ427に移る。ステップ426では、管理コマンドの処理が正常に終了したことをホスト機器160に示すため、正常終了(例えば、9000h)というステータスコードを含むレスポンスAPDU512を作り、ステップ427に移る。

【0071】

ステップ427では、レスポンスAPDU512からセキュアリードデータ511を作成する。この後、ホスト機器160はセキュアリードコマンドを発行し

(428)、コントローラチップ120はセキュアリードデータ511を出力する(429)。そして、ホスト機器160はセキュアリードデータ511を受信する(430)。

【0072】

尚、本発明は、カード形式以外の記憶装置にも適用可能である。

【0073】

【発明の効果】

本発明によれば、ICカードチップのアプレットごとにメモリの異なるブロックを割り当てることにより、ICカードチップのアプレット間のデータ干渉、即ち、あるアプレットに割り当てられたメモリが他のアプレットにもアクセスされてデータが侵害されることを抑制できるという効果を奏する。

【図面の簡単な説明】

【図1】 本発明を適用したMMCの内部構成を示す図である。

【図2】 コントローラチップとICカードチップとの間のICカードコマンドおよびICカードレスポンスの構造を示す図である。

【図3】 ICカードチップからの要求に応じてフラッシュメモリチップ上のセキュアデータエリアに対するデータの読み書きを実行するフローチャートである。

【図4】 ICカードチップからの要求に応じてフラッシュメモリチップ上の管理エリアに対するアプレットの登録およびその解除、また登録情報のロックおよびアンロックを実行するフローチャートである。

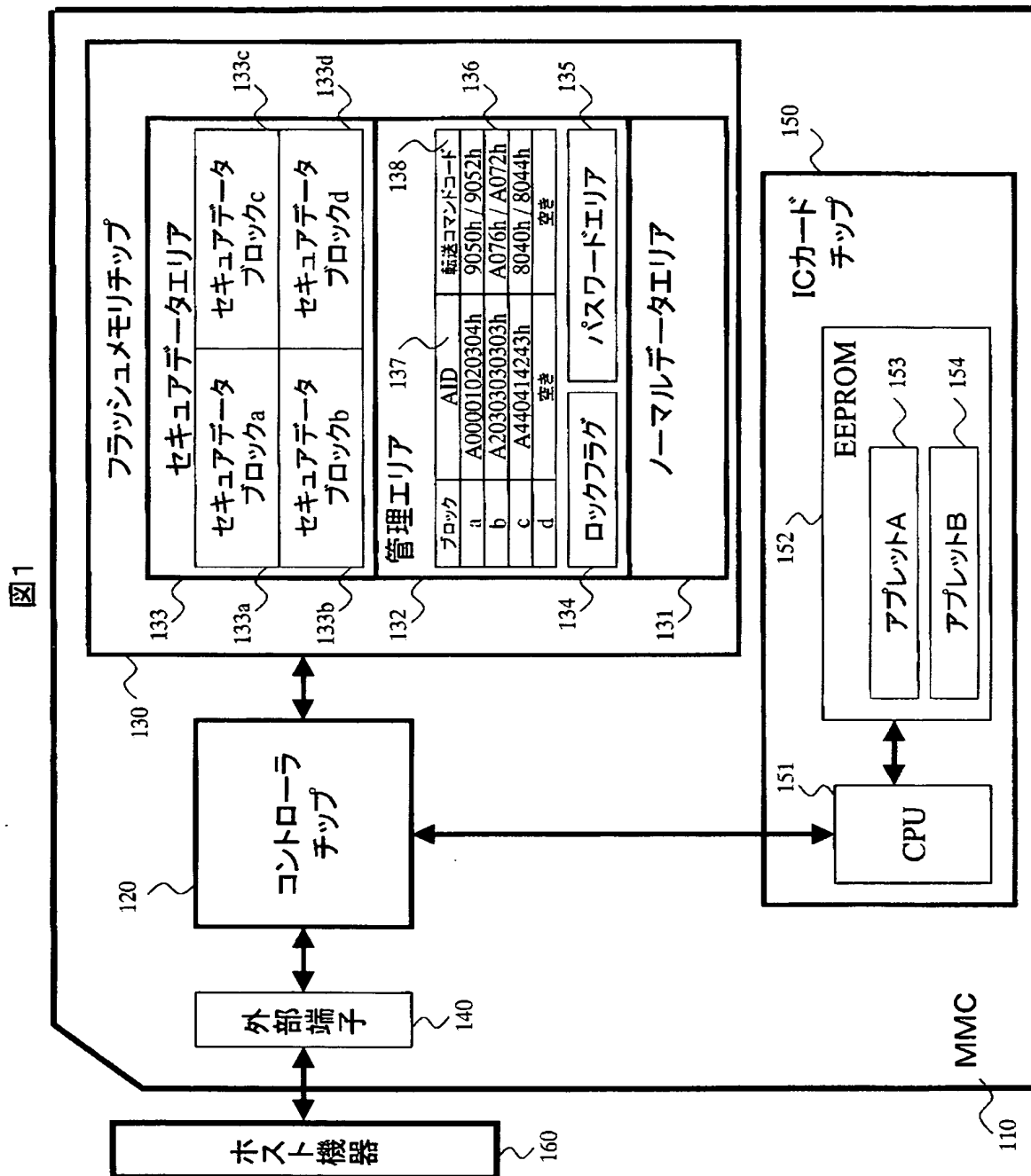
【図5】 セキュアライトデータとセキュアリードデータの構成図である。

【符号の説明】

110…MMC、120…コントローラチップ、136…管理テーブル、140…MMC外部端子、150…ICカードチップ、160…ホスト機器。

【書類名】 図面

【図 1】



【図 2】

図 2

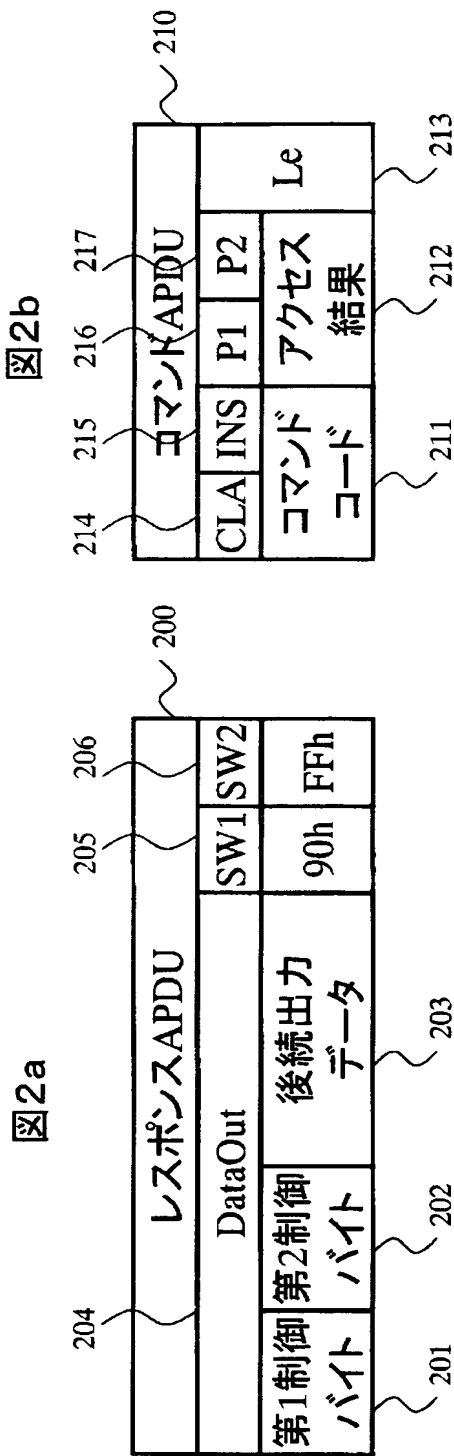
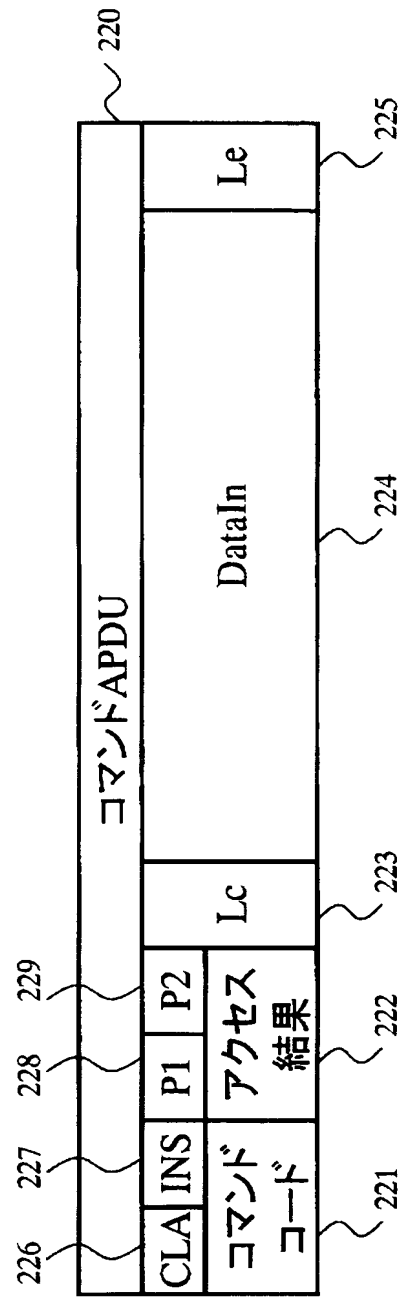
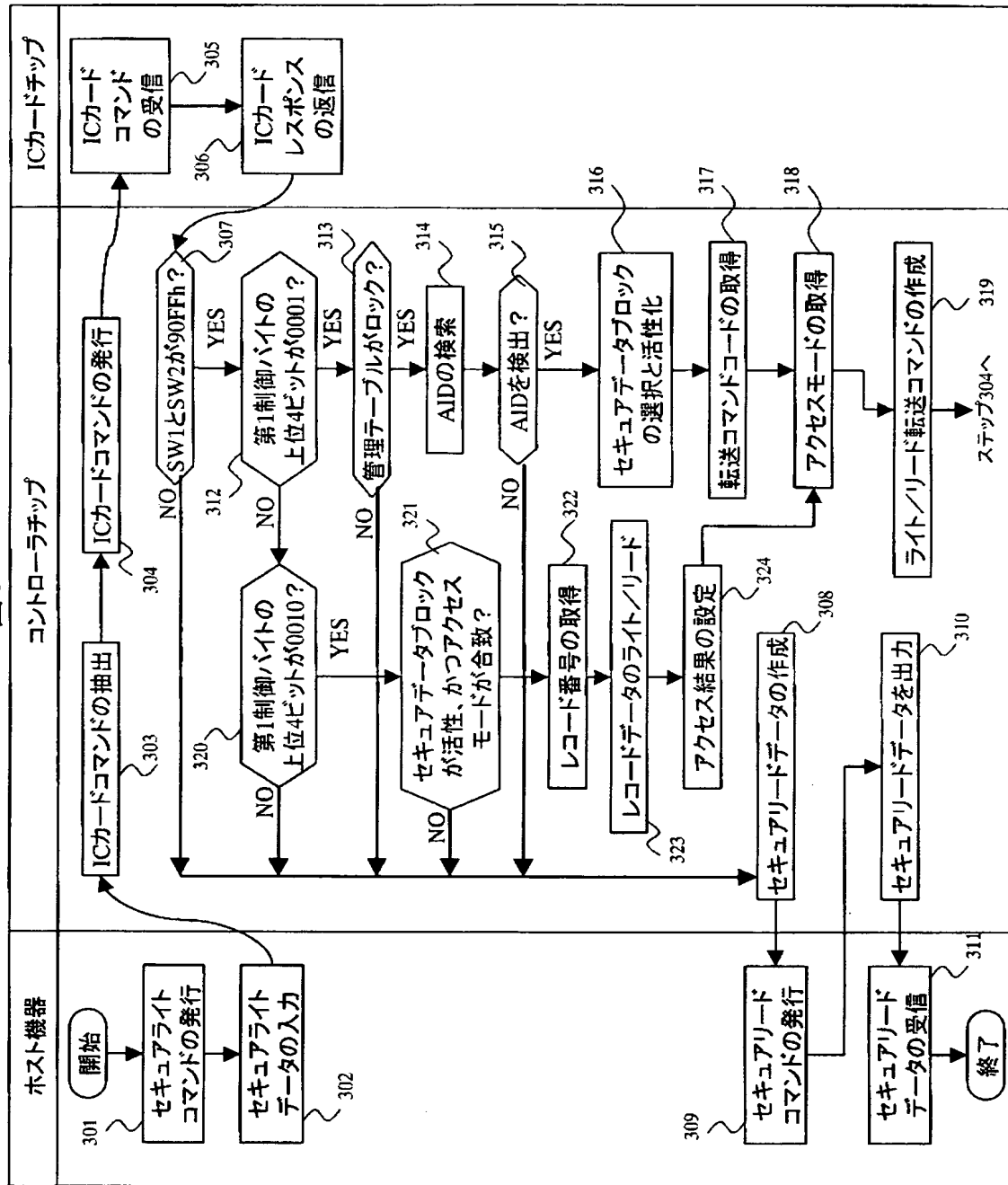


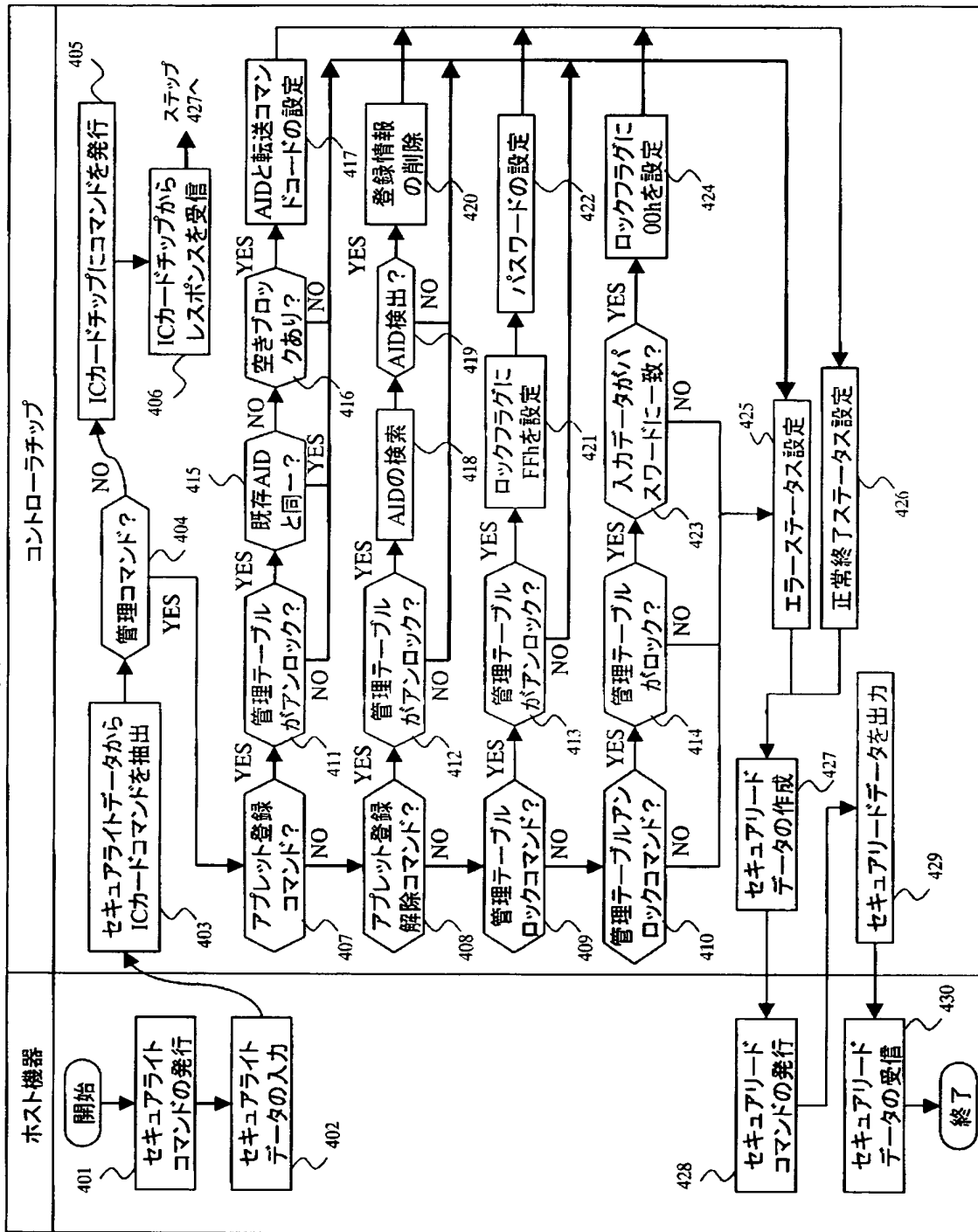
図 2c



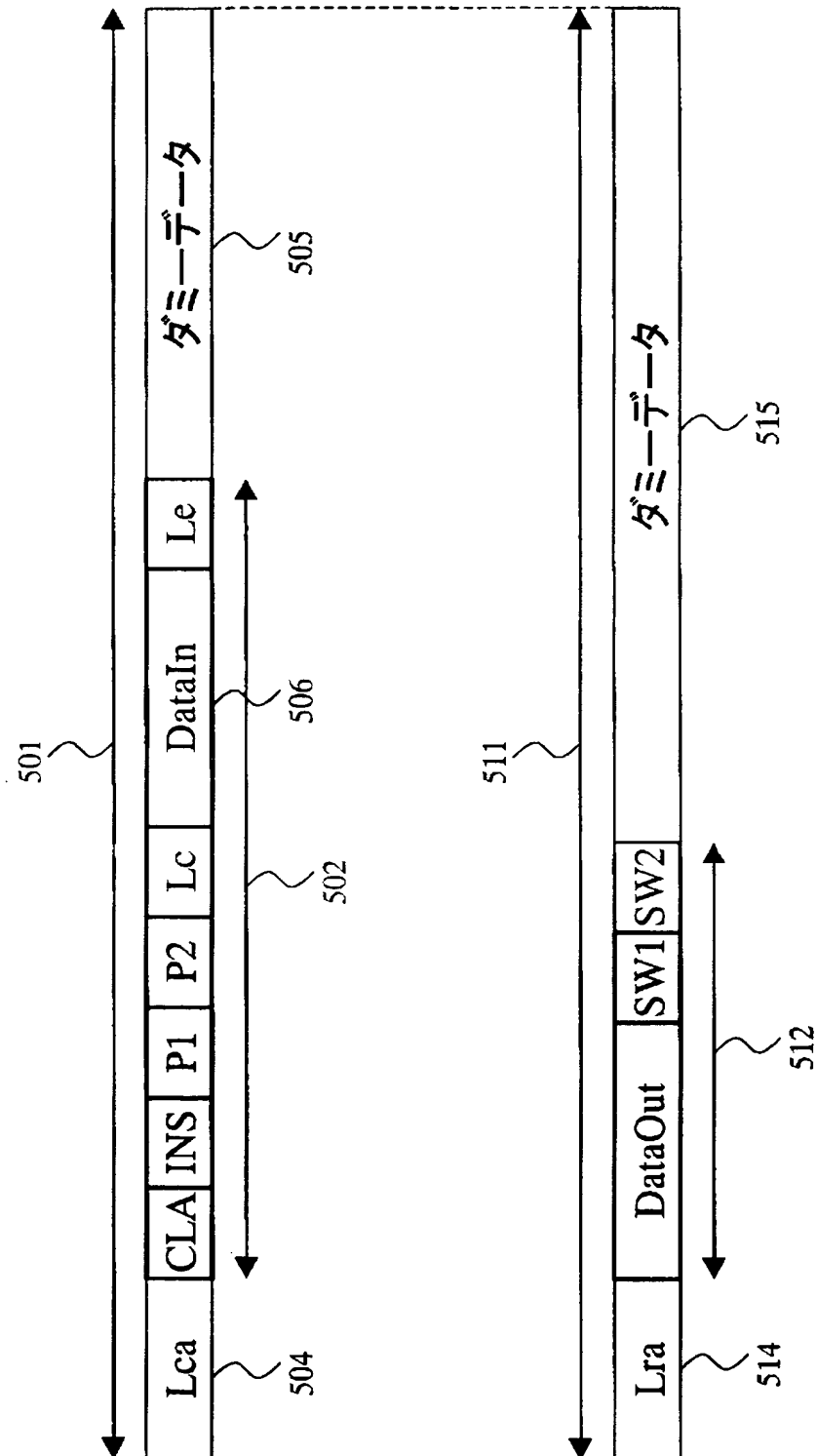
【図 3】



【図 4】



【図 5】



【書類名】 要約書

【要約】

【課題】

ＩＣカードチップのアプレット間のデータ干渉、即ち、一のアプレットに割り当てられたメモリが他のアプレットにもアクセスされてデータが侵害されることを抑制する。

【解決手段】

本発明は、フラッシュメモリチップ１３０と、ＩＣカードチップ１５０と、ホストからの要求に応じてフラッシュメモリチップ及びＩＣカードチップへのデータの読み書きを制御するコントローラチップ１２０とを備え、フラッシュメモリチップは、ホスト機器からのデータを記憶するためのノーマルデータエリア１３１とＩＣカードチップからのデータを記憶するためのセキュアデータエリア１３３を有し、さらに、セキュアデータエリア１３３は、アプレット１５３、１５４ごとに割り当てられたセキュアデータブロック１３３ａ，１３３ｂ，１３３ｃ，１３３ｄに分割される。

【選択図】 図１

認定・付加情報

特許出願の番号	特願 2 0 0 3 - 0 2 8 9 9 8
受付番号	5 0 3 0 0 1 8 7 6 8 5
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 5 年 2 月 7 日

< 認定情報・付加情報 >

【提出日】	平成15年 2月 6日
-------	-------------

次頁無

【書類名】 出願人名義変更届（一般承継）

【あて先】 特許庁長官 殿

【事件の表示】

【出願番号】 特願2003- 28998

【承継人】

【識別番号】 503121103

【氏名又は名称】 株式会社ルネサステクノロジ

【承継人代理人】

【識別番号】 100080001

【弁理士】

【氏名又は名称】 筒井 大和

【提出物件の目録】

【包括委任状番号】 0308729

【物件名】 承継人であることを証明する登記簿謄本 1

【援用の表示】 特許第 3 1 5 4 5 4 2 号 平成 1 5 年 4 月 1 1 日付け
提出の会社分割による特許権移転登録申請書 を援用
する

【物件名】 権利の承継を証明する承継証明書 1

【援用の表示】 特願平 1 - 2 5 1 8 8 9 号 同日提出の出願人
名義変更届（一般承継）を援用する

【プルーフの要否】 要

認定・付加情報

特許出願の番号	特願 2003-028998
受付番号	50301403515
書類名	出願人名義変更届（一般承継）
担当官	小野寺 光子 1721
作成日	平成15年11月 4日

<認定情報・付加情報>

【提出日】 平成15年 8月26日

特願 2 0 0 3 - 0 2 8 9 9 8

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 1 0 8]

1. 変更年月日	1 9 9 0 年 8 月 3 1 日
[変更理由]	新規登録
住 所	東京都千代田区神田駿河台 4 丁目 6 番地
氏 名	株式会社日立製作所

特願 2 0 0 3 - 0 2 8 9 9 8

出 願 人 履 歴 情 報

識別番号

[5 0 3 1 2 1 1 0 3]

1. 変更年月日

2 0 0 3 年 4 月 1 日

[変更理由]

新規登録

住 所

東京都千代田区丸の内二丁目 4 番 1 号

氏 名

株式会社ルネサステクノロジ